EXHIBIT 2

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **12/838,999**

Applicant: **LAMBERT, Robert John**

Filed: **July 19, 2010**

Title: **SYSTEM AND METHOD FOR REDUCING THE COMPUTATION AND STORAGE REQUIREMENTS FOR A MONTGOMERY-STYLE REDUCTION**

Art Unit: **2448**

Examiner: **WHIPPLE, Brian P.**

Docket No.: **67539/01022**

Mail Stop AF
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE AFTER FINAL REJECTION

Sir:

This is further to the Office Action dated March 22, 2013. Applicant wishes to present the following remarks:

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 6 of this paper.

OK TO ENTER: /B.W./

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.:	**12/838,999**
Applicant:	**LAMBERT, Robert John**
Filed:	**July 19, 2010**
Title:	**SYSTEM AND METHOD FOR REDUCING THE COMPUTATION AND STORAGE REQUIREMENTS FOR A MONTGOMERY-STYLE REDUCTION**
Art Unit:	**2448**
Examiner:	**WHIPPLE, Brian P.**
Docket No.:	**67539/01022**

Mail Stop AF
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE AFTER FINAL REJECTION

Sir:

This is further to the Office Action dated March 22, 2013. Applicant wishes to present the following remarks:

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 6 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for performing, on a cryptographic apparatus, a Montgomery-style reduction in a cryptographic operation, the method comprising:

obtaining an operand for the cryptographic operation ~~a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction~~;

computing a modified operand ~~by applying the~~ using a ~~modified~~ reduction value, instead of [[the]] a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and

outputting the modified operand.

2. (currently amended) The method according to claim 1 wherein the ~~modified~~ reduction value is $n' = 2^{-w} \bmod n$, or a shifted or signed version of n', w corresponds to a word size, and n corresponds to the modulus.

3. (currently amended) The method according to claim 1, wherein the computing further comprises:

successively applying the ~~modified~~ reduction value to perform a replacement of each of the second least significant word of the operand through the second most significant word of the operand; and

performing a standard Montgomery reduction on the most significant word of the operand.

4. (original) The method according to claim 3, wherein the performing a standard Montgomery reduction comprises storing a precomputed value μ in a register, using the value μ in computing another value m, and overwriting the register with m.

5. (original) The method according to claim 1, wherein the cryptographic apparatus comprises a Montgomery engine configured to perform the cryptographic operation.

6. (currently amended) The method according to claim 1, wherein the ~~modified~~ reduction value is pre-computed and stored with one or more cryptographic system parameters prior to the computing.

7. (original) The method according to claim 1, wherein the performing comprises zeroing the least significant word of the operand, modifying one or more remaining words, and shifting one or more modified words, wherein the shifting is either logical or physical.

8. (original) The method according to claim 7, wherein if a carry is produced during the computing, the outputting comprises adding the carry as a most significant word in the modified operand.

9. (original) The method according to claim 1, wherein said cryptographic operation comprises multiplication or squaring.

10. (currently amended) A cryptographic apparatus comprising a processor configured to operate as a Montgomery engine, and computer executable instructions that when executed by the processor:

obtain an operand for the cryptographic operation ~~a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction~~;

compute a modified operand ~~by applying the~~ using a ~~modified~~ reduction value, instead of [[the]] a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and

output the modified operand.

11. (currently amended) The apparatus according to claim 10, wherein said ~~modified~~ reduction value is $n' = 2^{-w} \bmod n$, or a shifted or signed version of n', w corresponds to a word size, and n corresponds to the modulus.

12. (currently amended) The apparatus according to claim 10, wherein the computing further comprises:

successively applying the ~~modified~~ reduction value to perform a replacement of each of the second least significant word of the operand through the second most significant word of the operand; and performing a standard Montgomery reduction on the most significant word of the operand.

13. (original) The apparatus according to claim 12, wherein performing a standard Montgomery reduction comprises storing a precomputed value μ in a register, using the value μ in computing another value *m*, and overwriting the register with *m*.

14. (currently amended) The apparatus according to claim 10, wherein the ~~modified~~ reduction value is pre-computed and stored with one or more cryptographic system parameters prior to the computing.

15. (original) The apparatus according to claim 10, wherein the performing comprises zeroing the least significant word of the operand, modifying one or more remaining words, and shifting one or more modified words, wherein the shifting is either logical or physical.

16. (original) The apparatus according to claim 15, wherein if a carry is produced during the computing, the apparatus is configured to add the carry as a most significant word in the modified operand.

17. (original) The apparatus according to claim 10, wherein the cryptographic operation comprises multiplication or squaring.

18. (currently amended) A non-transitory computer readable medium comprising computer executable instructions that when executed by a cryptographic apparatus, cause the cryptographic apparatus to:

obtain an operand for the cryptographic operation ~~a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction~~;

compute a modified operand ~~by applying the~~ using a ~~modified~~ reduction value, instead of [[the]] a modulus used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof, the reduction value being a function of the modulus; and

output the modified operand.

19. (currently amended) The non-transitory computer readable medium according to claim 18, wherein said ~~modified~~ reduction value is $n' = 2^{-w} \bmod n$, or a shifted or signed version of n', *w* corresponds to a word size and *n* corresponds to the modulus.

20. (currently amended) The non-transitory computer readable medium according to claim 18, wherein the computing further comprises:

successively applying the ~~modified~~ reduction value to perform a replacement of each of the second least significant word of the operand through the second most significant word of the operand; and

performing a standard Montgomery reduction on the most significant word of the operand.

21. (previously presented) The non-transitory computer readable medium according to claim 20, wherein performing a standard Montgomery reduction comprises storing a precomputed value μ in a register, using the value μ in computing another value *m*, and overwriting the register with *m*.

22. (currently amended) The non-transitory computer readable medium according to claim 18, wherein the ~~modified~~ reduction value is pre-computed and stored with one or more cryptographic system parameters prior to the computing.

23. (previously presented) The non-transitory computer readable medium according to claim 18, wherein the performing comprises zeroing the least significant word of the operand, modifying one or more remaining words, and shifting one or more modified words, wherein the shifting is either logical or physical.

24. (previously presented) The non-transitory computer readable medium according to claim 23, wherein if a carry is produced during the computing, executing instructions to add the carry as a most significant word in the modified operand.

25. (previously presented) The non-transitory computer readable medium according to claim 18, wherein the cryptographic operation comprises multiplication or squaring.

REMARKS

Applicant thanks the Examiner for reviewing the present application. The claims have been amended only to clarify the protection being sought. Claim 1 has been amended to clarify that the operand is obtained and the modified operand computed using the reduction value. The term "modified" has been removed to improve clarity and the features from the previous "obtaining" operation have been moved into the "computing" operation. Claims 2, 3, 6, 10-12, 14, 18-20, and 22 have been amended in a consistent manner. Applicant respectfully submits that no new subject matter has been added.

Claims 1, 3, 5-10, 12, 14-18, 20, and 22-25 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sabin (EP 1,818,809) in view of Gopal (U.S. Publication No. 2010/0332578). Claims 2, 11, and 19 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sabin and Gopal, in further view of Romain (U.S. 6,424,987). Claims 4, 13, and 21 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sabin and Gopal, in further view of Applicant Admitted Prior Art (AAPA). Applicant respectfully traverses the rejections as follows.

Claim 1 recites in part:

> "obtaining an operand for the cryptographic operation;
>
> computing a modified operand using <u>a reduction value</u>, <u>instead of a modulus</u> used in performing a standard Montgomery reduction, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof<u>, the reduction value being a function of the modulus</u>" [emphasis added].

Applicant respectfully submits that the Examiner has either misconstrued the teachings of the cited references or has read too much into these references. None of the cited references teach or suggest using a reduction value instead of a modulus, let alone one that is a function of a modulus used in a standard Montgomery reduction.

As discussed in paragraphs [0028] to [0030] of the application as filed, to improve the reduction efficiency of a Montgomery machine, the objective should be to reduce the number of operations, especially word-by-word multiplication, and to maximize the number of components that can be kept in registers, reducing the loading and storing of temporary values.

In the present application, a system and method are described that provide an alternative way in which to produce a Montgomery reduction from below by storing a new precomputed value used to substantially replace the μ and n values used in a standard Montgomery reduction with a single value.

This may be done by storing a reduction value in the cryptographic apparatus, wherein the reduction value, when applied to an operand, input to or generated by, the cryptographic apparatus, performs a replacement for values in a low-order segment which is a target of the reduction, rather than a cancellation thereof, as performed in a standard Montgomery reduction; and performing the reduction from below using the reduction value.

By modifying the Montgomery reduction mechanism in this way, the number of multiplications and registers required to effect the Montgomery reduction can be reduced. In other words, not only is the claimed method used to perform a reduction differently, a reduction value is used, as clearly recited in claim 1.

Sabin may discuss details of a Montgomery Reduction. However, Sabin does not teach or suggest the use of a reduction value, let alone as recited in claim 1. At most, Sabin teaches a modified Montgomery-related process. The Montgomery reduction discussed in Sabin includes details of a standard Montgomery reduction. There is no discussion by Sabin of a reduction value, let alone such a value that is a function of the modulus. For example, paragraphs [00157] through [00162] of Sabin, which have been relied upon by the Examiner, clearly teach a normal Montgomery Reduction. There is no discussion by Sabin of modifying the reduction, let alone using a reduction value instead of the modulus. In fact, it is unclear from the Examiner's rejection what in Sabin is being equated to the reduction value in claim 1.

The Examiner has acknowledged that: "Sabin is silent on the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction" and cites Gopal as teaching what is missing from Sabin. Sabin therefore fails to teach or suggest both a reduction value, and how such a value is derived. In any event, Gopal also fails to teach or suggest a reduction value. Accordingly, Applicant respectfully submits that the cited references fail to teach each and every element of claim 1 and, as such, a *prima facie* case of obviousness has not been established.

Gopal teaches, among other things, a side-channel safe modular reduction that uses an iterative folding scheme based on a modified Barret's Algorithm. Although Gopal may teach modifying a Montgomery reduction process, this is done by using an iterative folding scheme, not by using a reduction value. Therefore, at most, Gopal teaches a modified Montgomery process. A modified process cannot be considered equivalent to a reduction value unless the process is modified using such a value. In the case of Gopal, the process is modified using a modified folding scheme. For at least that reason, Applicant respectfully submits that Gopal fails to make up for what is missing in Sabin and thus claim 1 is patentable over Sabin in view of Gopal.

With respect to Romain, Applicant respectfully submits that the Examiner is reading too much into the teachings relied upon. Particularly, Applicant notes that the expression $I = 2^{-n} \bmod N$ on line 37 of column 1 is not equivalent to the reduction value described in the present application. First, in Romain, I is a binary data element called an error. There is nothing in Romain that suggests the form of the error could be applied to a reduction value. In fact, Romain does not teach or suggest a reduction value. Second, $I = 2^{-n} \bmod N$ does not incorporate the word size, as is recited in claim 2 (i.e. *w*), the number of bits *n* is used. Finally, $I = 2^{-n} \bmod N$ appears to be reduced by a binary data element N. Romain does not suggest that the value N is the modulus and thus does not teach what is missing from Sabin and Gopal.

For at least these reasons, Applicant respectfully submits that the claims are also patentable over Sabin and Gopal, in further view of Romain.

With respect to AAPA, although Figure 3 of the present application illustrates a standard Montgomery reduction, there is nothing in the present application that suggests performing a standard Montgomery reduction on the most significant word of the operand after applying the reduction value as recited in claim 3, is part of the prior art.

For at least the above reasons, Applicant respectfully submits that claims 1-25 are patentable over the cited references.

In view of the foregoing, Applicant respectfully submits that the present application is in condition for allowance and therefore requests early reconsideration and allowance of the present application.

Respectfully submitted,

Brett J. Slaney
Agent for Applicant
Registration No. 58.772

Date: May 1, 2013

BLAKE, CASSELS & GRAYDON LLP
199 Bay Street
Suite 4000, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-2518
BS/